November 2015

CRITICAL INFRASTRUCTURE PROTECTION

Sector-Specific Agencies Need to Better Measure Cybersecurity Progress

GAO Highlights

Highlights of GAO-16-79, a report to the Committee on Homeland Security, House of Representatives

Why GAO Did This Study

U. S. critical infrastructures, such as financial institutions, commercial buildings, and energy production and transmission facilities, are systems and assets, whether physical or virtual, vital to the nation's security, economy, and public health and safety. To secure these systems and assets, federal policy and the NIPP establish responsibilities for federal agencies designated as SSAs, including leading, facilitating, or supporting the security and resilience programs and associated activities of their designated critical infrastructure sectors.

GAO's objectives were to determine the extent to which SSAs have (1) identified the significance of cyber risks to their respective sectors' networks and industrial control systems, (2) taken actions to mitigate cyber risks within their respective sectors, (3) collaborated across sectors to improve cybersecurity, and (4) established performance metrics to monitor improvements in their respective sectors. To conduct the review, GAO analyzed policy, plans, and other documentation and interviewed public and private sector officials for 8 of 9 SSAs with responsibility for 15 of 16 sectors.

What GAO Recommends

GAO recommends that certain SSAs collaborate with sector partners to develop performance metrics and determine how to overcome challenges to reporting the results of their cyber risk mitigation activities. Four of these agencies concurred with GAO's recommendation, while two agencies did not comment on the recommendations.

View GAO-16-79. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Sector-specific agencies (SSA) determined the significance of cyber risk to networks and industrial control systems for all 15 of the sectors in the scope of GAO's review. Specifically, they determined that cyber risk was significant for 11 of 15 sectors. Although the SSAs for the remaining four sectors had not determined cyber risks to be significant during their 2010 sector-specific planning process, they subsequently reconsidered the significance of cyber risks to the sector. For example, commercial facilities sector–specific agency officials stated that they recognized cyber risk as a high-priority concern for the sector as part of the updated sector planning process. SSAs and their sector partners are to include an overview of current and emerging cyber risks in their updated sector-specific plans for 2015.

SSAs generally took actions to mitigate cyber risks and vulnerabilities for their respective sectors. SSAs developed, implemented, or supported efforts to enhance cybersecurity and mitigate cyber risk with activities that aligned with a majority of actions called for by the National Infrastructure Protection Plan (NIPP). SSAs for 12 of the 15 sectors had not identified incentives to promote cybersecurity in their sectors as proposed in the NIPP; however, the SSAs are participating in a working group to identify appropriate incentives. In addition, SSAs for 3 of 15 sectors had not yet made significant progress in advancing cyber-based research and development within their sectors because it had not been an area of focus for their sector. Department of Homeland Security guidance for updating the sector-specific plans directs the SSAs to incorporate the NIPP's actions to guide their cyber risk mitigation activities, including cybersecurity-related actions to identify incentives and promote research and development.

All SSAs that GAO reviewed used multiple public-private and cross-sector collaboration mechanisms to facilitate the sharing of cybersecurity-related information. For example, the SSAs used councils of federal and nonfederal stakeholders, including coordinating councils and cybersecurity and industrial control system working groups, to coordinate with each other. In addition, SSAs participated in the National Cybersecurity and Communications Integration Center, a national center at the Department of Homeland Security, to receive and disseminate cyber-related information for public and private sector partners.

The Departments of Defense, Energy, and Health and Human Services established performance metrics for their three sectors. However, the SSAs for the other 12 sectors had not developed metrics to measure and report on the effectiveness of all of their cyber risk mitigation activities or their sectors' cybersecurity posture. This was because, among other reasons, the SSAs rely on their private sector partners to voluntarily share information needed to measure efforts. The NIPP directs SSAs and their sector partners to identify high-level outcomes to facilitate progress towards national goals and priorities. Until SSAs develop performance metrics and collect data to report on the progress of their efforts to enhance the sectors' cybersecurity posture, they may be unable to adequately monitor the effectiveness of their cyber risk mitigation activities and document the resulting sector-wide cybersecurity progress.